High-Availability User Networks

0490 By extension of the PBSN concept, using the Data Replication Agent software element, a computer user can have, invisibly, multiple local and remote copies of the all of the user's important data made on the PBSN (see Figure 15). By this means, any user that suffers a computer failure can access data immediately through any other computer on the PBSN. This method can be extended to encompass a full image of the user's working data, so that building a new computer can be accomplished in a very short time by simply copying that image from the PBSN to the new computer. These features are a part of the PBSN agent's Data Replication Agent function.

0500 Since the DEA system uses very long encryption keys, which are not memorisable, to provide the encryption capability, it is necessary to provide a means to store these keys in case of the failure of a user's computer. A number of methods are available to achieve this, ranging from physical keys such as security cards, smart cards or keys or even microchips embedded under the skin, to logical access systems using passwords or lookup files, among other means. Several of these means have some level of security exposure. The DEA and the other software elements of the invention are designed to support a variety of these means, allowing for different levels of security in the installed product.

Alternative Implementations of the Invention

0510 An alternative method (Figure 16) of building the SNAS system is to install the DAC, the ARD and some of the other software facilities on a network switching device, such as a SAN, LAN or Wide Area Network switch, hub or router; so effectively making the redirections within that switching device and effectively invisible in most circumstances to the client computers.

CLAIMS

What I claim are:

1) A means of building a Scalable Network-Attached Storage system where control of the data storage elements of said system is distributed over the computer elements of said system, so allowing said computer elements to access and control said data elements in a shared fashion whereby:

a) Control of the data-storage sub-elements of a data storage element can reside in different computer elements, so allowing large numbers of computer elements to be used in the Scalable Network-Attached Storage system, and so allowing said system to be easily and economically expanded in size and performance and reconfigured to needs;

b) Control of any such data storage sub-element can be replicated in several computer elements in such a way that these several computer elements can access said data sub-elements;

c) Allocation to the set of computer elements of said control of access to said data elements and data sub-elements is initially established by a software functionality according to a set of user and computer generated policy rules; and where said software functionality adjusts said distribution of access control across said computer elements on a periodic basis, depending on metrics measured periodically throughout the Scalable Network-Attached Storage system

d) Computer elements are specifically designated as the initial contact point for a client computer to the Scalable Network-Attached storage system, which designated computer elements have a software facility to determine that computer element having control of the data storage element that said client computer wishes to access and by means of said software facility re-direct said client computer to communicate directly with that computer element;

e) Where the software facility of paragraph c) in Claim 1) above detects the addition of new computer elements to the Scalable Network-Attached Storage system via the periodic metrics transmitted to said software facility by said new computer element; and thereby said software facility re-maps the allocation to said computer elements of access control of said data storage elements to make use of said new computer element; and where the loss of a computer element through failure or removal is detected by a loss of periodic metric data, so causing said software facility to re-map the allocation to the remaining computer elements of access control of those data storage elements previously controlled by said lost computer element;

2) An extension of the means of Claim 1) where temporary loss of access to said data storage elements is reduced by having a prepared backup map of the Scalable Network-Attached Storage system, whereby another backup computer element, which is configured to rapidly

take control of said data elements, is designated for each computer element in such a way that a hardware or software failure will not affect both said computer element and its designated backup simultaneously; so that a failure detected by the software facility in Para e) of Claim 1) will cause that software facility to move control to said backup computer element;

And where said backup computer element may be a computer element or one of a set of computer elements specifically and solely functioning as backup computer elements;

Or where said backup computer element may be a computer element that is actively controlling access to other data storage elements.

3) An extension to the means of Claim 1) where the performance of the Scalable Network-Attached Storage system is increased by mapping multiple computer elements to be able to control any given data storage element;

Where one of said controlling computer elements is designated as the sole computer element allowed to change said data storage element, with the other computer elements being able to read said data storage element; or where the type of data storage element or the client computers' method of accessing same permits multiple computer elements to change said data storage element.

4) An extension to Claim 3 whereby the ability of the system to recover from a failure is enhanced by having a data replication software facility which allows a computer element to replicate data according to policy rules managed by the system, with said replication being to both local computer elements who store such replicas on the data storage elements under their control, or to remote computer elements, permitting copies of data to be at a safe distance to protect against natural or man-made disasters;

And where said data replication software facility may also be used to provide copies of data at the remote site or sites for said remote site or sites to be able to access data more rapidly than if it were at the originating site;

And where the said policy rules for replication may include schedule, frequency and priority of replication, number of backup copies, type of backup data storage elements and other policy rules.

5) An extension of Claim 1 above whereby a two-tier system is used to mange unused free space in the Scalable Network-Attached Storage system and its derivatives, such two-tier

system being implemented as a software facility that provides both a means to allocate part of the available unused free space to each computer element, keeping the remainder under its own control, and which software facility uses policy rules to monitor, control and change this allocation periodically based on metric information reported to said software facility by the computer elements.

6) An extension to the means in the above claims whereby a set of the data storage elements and computer elements in a Scalable Network-Attached Storage system are designated as a Secure Scalable Network-Attached Storage system, with the data storage elements being encrypted by the client computer, and with the file structure of said data elements being encrypted, and with communications between the client systems and the Scalable-Network-Attached storage system being encrypted.

7) An extension to the means in the above claims whereby those means are employed to take advantage of data storage elements in the client computers by using said data storage elements in part or in whole as data storage elements in a distributed form of Scalable Network-Attached Storage (here named Peer-Based Storage Network), where

   a) The data storage elements in any given client computer can be shared with other client computers under the control of the Scalable Network-Attached Storage software forming this invention, as extended to provide the Peer-Based Storage network capability, and with the features of replication and security as claimed above and described herein;

   b) Where software facilities are provided to allow designation of the amount of said data storage elements a client computer may wish to share; with software facilities to increase or decrease said amount as desired without causing loss of data to the client computers sharing the data storage elements being changed;

   c) Where replication and backup policies may be developed to protect automatically against loss of a client computer and/or its stored data on its data storage elements

8) An alternative construction of the invention whereby the computer elements of the Scalable Network-Attached Storage system, Secure Scalable Network-Attached Storage system or Peer-Based Storage Network in part or in whole are replaced by a storage network switching element or a local area network switching element or a communications switching element.